использования данных АЗ сильно снижается.

Закладные устройства, изменяющие протокол передачи данных, очевидно, целесообразно использовать в таких устройствах, как модемы и сетевые карты. При этом данные АЗ могут осуществлять трансляцию передаваемой информации третьей стороне. Как уже отмечалось выше, в случае использования алгоритмов закрытия передаваемой информации эффективность от использования данных АЗ резко падает.

Говоря о сертификации сложных электронных систем на соответствие специфицированным функциям необходимо отметить, что для осуществления сертификации необходимы аппаратно-программные средства.

Структура инструментальных средств представляет собой аппаратно-программный комплекс, в состав которого входят прикладное программное обеспечение и аппаратные средства сертификации. Программное обеспечение должно включать в себя среду моделирования, позволяющую создавать программные модели сертифицируемых устройств, а также получать тестирующие последовательности для осуществления диагностики. Прикладное программное обеспечение должно выполнять следующие функции: инициализация комплекса; задание режимов работы; программная имитация внешней среды для исследуемого объекта; запись в аппаратную часть комплекса тестирующих последовательностей для исследуемого объекта; анализ результатов (обработка и анализ временных диаграмм, полученных от исследуемого объекта). Аппаратная часть комплекса предназначена для выполнения следующих функций: обеспечение аппаратной поддержки прикладного программного комплекса; реализация взаимодействия с исследуемым объектом в режиме реального времени; регистрация состояния и физическая эмуляция внешней среды исследуемой электронной системы.

III Выводы

В заключение хотелось бы отметить, что в данной работе исследуется проблема защиты информации от угроз, исходящих от аппаратных ресурсов КС. Рассматриваются источники угроз, размещение которых возможно как непосредственно в интегральных схемах ЭВМ, так и в периферийном оборудовании. Понятие «закладное устройство», определённое в ДСТУ [5], в работе без изменения сути трактуется как аппаратная закладка. Угроза информации осуществляется за счёт не специфицированных функций электронных систем. Приведём несколько важных характеристик АЗ: установить источник угроз невозможно без специальных инструментальных средств; контроль за угрозами аппаратного уровня невозможно осуществлять на программном уровне.

Эти и другие характеристики делают АЗ очень перспективным компонентом компьютерных диверсий, в том числе, в форме нарушения работы важных государственных и коммерческих систем.

Литература: 1. Анин Борис. Защита компьютерной информации. – СПб.: BHV Санкт-Петербург, 2000. VIII. – 368 с.: ил. 2. Попов М. И. Основы сертификации электронной техники. – М.: Издательство стандартов, 1988. – 277 с. 3. Проскурин В. Г. и др. Программно-аппаратные средства обеспечения информационной безопасности. Защита в ОС. – М.: Радио и связь, 2000. – 166 с.: ил. 4. Защита информации: Сборник научных трудов / Киев, Международный университет гражданской авиации.– К: КНИГА, 1999.– 188 с. 5. ДСТУ 2226-93. Автоматизированные системы. Термины и определения.

УДК 681. 324

МЕТОДИКА СИСТЕМАТИЗАЦИИ ХАРАКТЕРИСТИК ТИПОВЫХ КОМПЬЮТЕРНЫХ СИСТЕМ, ВЛИЯЮЩИХ НА ЗАЩИТУ ИНФОРМАЦИИ

Игорь Яковив, Александр Черноног*, Павел Алексийчук*

*Национальная академия СБУ, *ВИТИ НТУУ «КПИ»*

Анотація: **Комп'ютерні системи для формування документів (типові комп'ютерні системи) знайшли широке поширення. Пропонується методика, що дозволяє систематизувати їх характеристики, найбільш важливі для захисту інформації від несанкціонованого доступу.**

Summary: **Computer systems for creation of the documents (the standard computer systems) have found a wide circulation. The technique permitting to systematize their performances, which is most significant for the protection of the information from unauthorized access is offered.**

Ключові слова: **Інформація, інформаційна безпека, комп'ютерна система, захист інформації.**

I Введение

Компьютерные системы (КС), специализация которых – подготовка традиционных документов, нашли широкое распространение в различных сферах деятельности. Для таких КС (далее – типовые КС) характерны некоторые особенности [1] (использование широко распространенных сетевых операционных систем и самодостаточный набор универсальных прикладных программ, сравнительно низкий уровень квалификации пользователей и другие), что позволяет:

- выработать единый комплексный подход по защите информации, априорно учитывающий особенности обработки файлов документов с помощью распространенного операционного и прикладного программного обеспечения;
- определить возможности и порядок применения в комплексных системах защиты информации (КСЗИ) штатных услуг сетевых операционных систем по защите и аудиту;
- конкретизировать и сделать более доступными для практического применения в типовых КС ряд положений нормативных документов системы технической защиты информации;
- разработать структуру типовой подсистемы управления КСЗИ, ее математическую модель и методики сравнения эффективности КСЗИ различной структуры;
- удешевить создание и эксплуатацию системы защиты информации для рассматриваемых КС.

Для составления типовой модели угроз, упрощения сравнительного анализа штатных услуг сетевых операционных систем по защите и аудиту, определения порядка их применения предлагается методика систематизации основных характеристик типовых КС, от которых зависит безопасность обрабатываемой информации.

Методика разрабатывалась для широко распространенного одномашинного многопользовательского комплекса, в котором поочередно обрабатывается информация одной или нескольких категорий конфиденциальности. Рассматриваемые подходы могут стать основой методики систематизации и для многомашинного многопользовательского комплекса с одновременной обработкой информации с ограниченным доступом.

II Порядок формирования документов

Основу методики составляет порядок формирования документов, представленный на рис. 1. Он включает наиболее значимые этапы, определяющие структуру и порядок функционирования КСЗИ.

1. Этап электронной обработки.

Данный этап включает два основных шага электронной обработки:

1) формирование файла документа;
2) формирование бумажного документа.

Целесообразно файлы документов систематизировать следующим образом [1]:

1) файл документа внутренний (ФДВн) – рабочий файл документа;
2) файл документа внешний (ФДВнш) – окончательно подготовленный для печати файл документа.

Можно выделить следующие способы формирования ФДВн:

- использование ранее созданного файла (-ов);
- создание нового файла.

Формирование бумажного документа осуществляется путем печати ФДВнш.

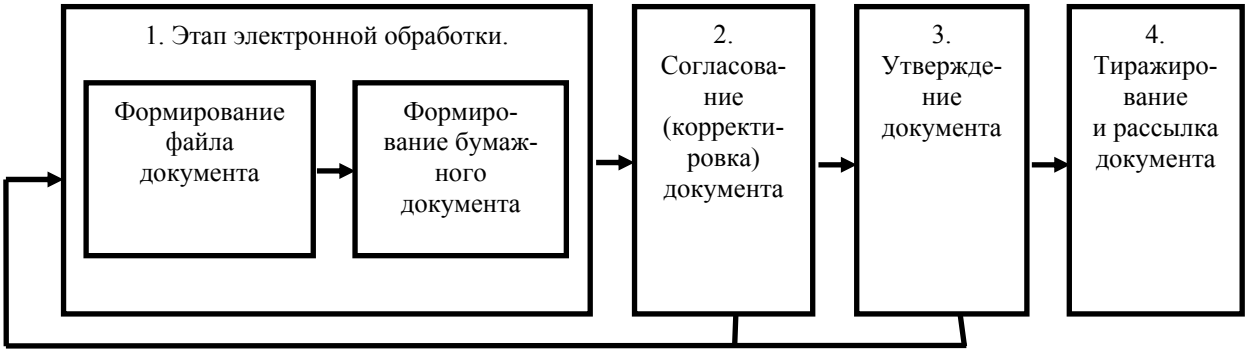

Рисунок 1 – Порядок формирования документов с помощью типовой компьютерной системы

2. Согласование (корректировка) документа.

Производится корректировка и подпись (согласование) сформированного пользователем бумажного

документа с вышестоящим руководством по инстанции. В случае внесения изменений документ возвращается на этап электронной обработки.

3. Утверждение документа.

Этап включает утверждение и подпись согласованного бумажного документа лицом, имеющим соответствующие полномочия (как правило – руководитель организации и его заместитель). В случае внесения изменений документ возвращается на этап электронной обработки.

4. Тиражирование и рассылка документа.

На данном этапе проводится размножение утвержденного документа и рассылка необходимого числа экземпляров.

Согласование и утверждение документа устраняют угрозы целостности документа. На этих же этапах становится маловероятной угроза нарушения конфиденциальности содержания документа, так как организационно просто обеспечивается доступ только тех лиц, которые имеют на это право. Наиболее вероятной становится угроза конфиденциальности содержанию документа на этапе электронной обработки за счет несанкционированного доступа другими пользователями КС.

III Порядок формирования файлов документов

Основные положения политики безопасности [1] для типовых КС следующие:

- перед началом работы пользователь регистрируется в машинном журнале (на бумажном носителе) и в ПК (ввод идентификатора и своего пароля);
- файлы документов пользователя формируются и хранятся только в именной выделенной папке. Доступ к папкам других пользователей запрещен организационными мерами и штатными средствами операционной системы (ОС);
- пользователь реализует свои функции с помощью установленных администратором приложений и программ;
- распечатка документов производится только на предварительно учтенных листах с фиксацией в машинном журнале;
- при необходимости сохранение файлов пользователя на учтенную дискету производит администратор; ввод данных с других носителей информации также осуществляется только через администратора;
- предусмотрен контроль над всеми действиями пользователей путем использования штатных средств аудита ОС; доступ пользователя к средствам аудита запрещен организационными мерами, а также механизмами защиты ОС.

В рамках такой политики безопасности этап электронной обработки можно представить следующей последовательностью действий пользователя ПК (рис. 2):

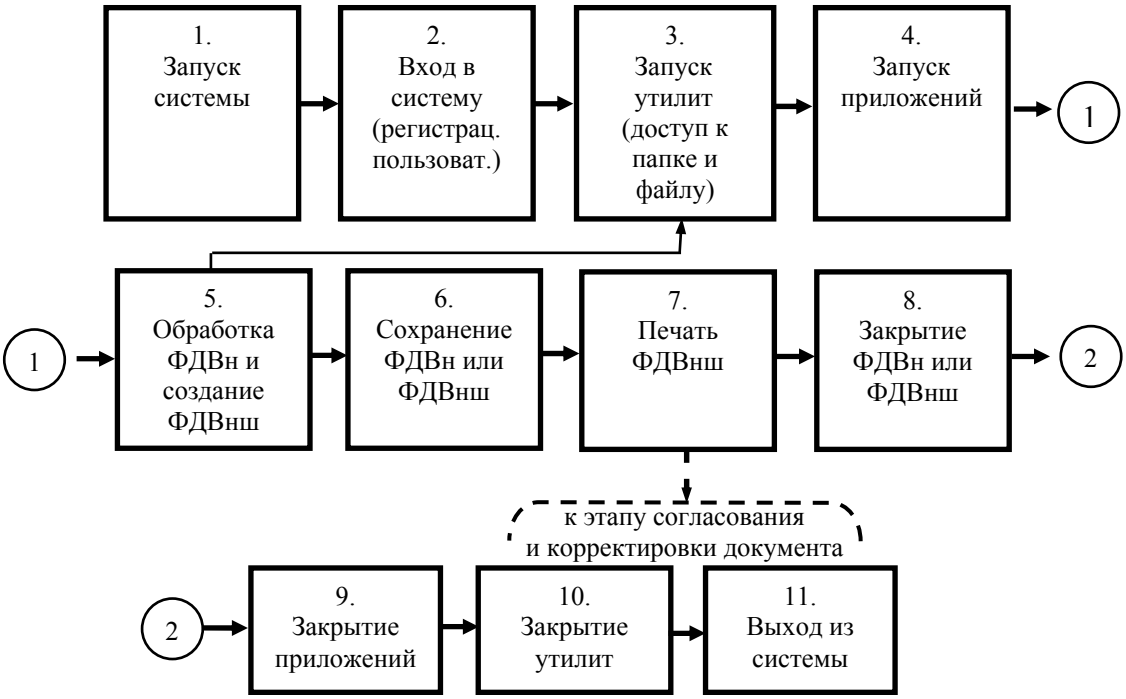

Рисунок 2 – Последовательность действий пользователя на этапе электронной обработки

- действиями операционной системы;
- возможными угрозами конфиденциальности информации и наблюдаемости за работой пользователя;

Результаты соответствия отражены в таблице 1, которая, по сути, представляет модель угроз, в деталях учитывающая особенности типовой КС и политики безопасности.

Таблица 1 – Соответствие действий пользователя, операционной системы и угроз (модель угроз)

Подэтапы электронной обработки	Действия пользователя	Действия ОС, приводящие к возникновению угроз	Угрозы
1	2	3	4
1. Запуск системы.	1. Запуск загрузки персонального компьютера путем включения питания.	1. Тесты BIOS. 2. Выполнение файлов загрузки.	1. Несанкционированное ознакомление с паролем BIOS. 2. Модификация параметров файлов загрузки.
2. Вход в систему (регистрация пользователя).	1. Действия согласно сценарию регистрации.	1. Выполнение файлов сценария регистрации.	1. Модификация параметров файлов сценария регистрации (в том числе, установок пароля). 2. Выполнение несанкционированных программ, имитирующих регистрацию пользователя.
3. Запуск утилит ОС (получение доступа к папкам и файлам)	1. Запуск необходимых для работы утилит. 2. Получение доступа к папкам и файлам.	1. Выполнение файлов запуска утилит в соответствии с полномочиями пользователя. 2. Предоставление доступа к папкам в соответствии с установленными в файлах доступа полномочиями: 1) просмотр списка; 2) чтение; 3) добавление; 4) добавление и чтение; 5) изменение; 6) полный доступ; 7) нет доступа; 8) создание; 9) удаление. 3. Предоставление доступа к файлам в соответствии с установленными в файлах доступа полномочиями: 1) чтение; 2) запись; 3) выполнение; 4) удаление; 5) изменение; 6) смена владельца; 7) полный доступ; 8) нет доступа; 9) восстановление; 10) просмотр файлов.	1. Модификация параметров доступа в файлах запуска утилит. 2. Модификация параметров доступа в файлах доступа пользователя.

Продолжение таблицы 1

4. Запуск приложений	1. Запуск необходимых для работы приложений.	1. Выполнение файлов запуска приложений в соответствии с полномочиями пользователя.	1. Модификация параметров доступа в файлах запуска приложений.
5. Обработка ФДВн и создание ФДВнш.	1. Запуск ранее созданного файла. 2. Создание нового ФДВн или ФДВнш. 3. Создание составного ФДВн или ФДВнш. 4. Удаление файла специальными утилитами.	1. Запуск файла при наличии полномочий в файлах доступа. 2. Создание нового файла. 3. Создание составного файла. 4. Удаление файла.	1. Модификация параметров доступа в файлах доступа пользователя. 2. Оставление пользователем файла в “корзине”. 3. Оставление пользователем возможности восстановления удаленного файла.
6.Сохранение ФДВн или ФДВнш.	1. Установка автосохранения. 2. Установка резервного копирования. 3. Сохранение в оперативной памяти (буфере обмена). 4. Сохранение файла в указанной папке. 5. Установка атрибутов сохранения.	1. Выполнение автосохранения. 2. Выполнение резервного копирования. 3 .Сохранение файла в оперативной памяти (буфере обмена). 4. Сохранение файла в указанной пользователем папке. 5. Сохранение файла с указанными пользователем атрибутами. 6. Сохранение файла в папке временных файлов. 7. Сохранение данных в файлах подкачки.	1. Доступ пользователя к папке хранения временных файлов. 2. Доступ пользователя к чужим данным, которые сохранены в оперативной памяти (буфере обмена). 3. Доступ пользователя к файлу подкачки. 4. Сохранение пользователем файла с запрещенными атрибутами доступа. 5. Бесконтрольное резервное копирование файлов.
7. Печать ФДВнш.	1. Запуск утилит печати. 2. Установка фоновой печати. 3. Контроль бумажных носителей при печати.	1 .Запуск утилит печати при наличии полномочий в файлах доступа. 2. Запуск фоновой печати. 3. Запись данных в буфер принтера печати.	1. Запрещенный запуск утилит печати. 2. Доступ пользователя к чужим данным фоновой печати. 3. Доступ пользователя к чужим данным буфера печати. 4. Печать на неучтенных носителях. 5. Выполнение запрещенного количества копий.
8. Закрытие ФДВн или ФДВнш.	1. Закрытие файла с сохранением данных. 2. Закрытие файла без сохранения данных.	1. Автоматическое сохранение файла независимо от пользователя.	1. Сохранение данных при закрытии независимо от пользователя. 2. Некорректное закрытие файла (например, при отсутствующем носителе данных).
9. Закрытие приложений.	1. Закрытие приложений.	1.Закрытие приложения без очистки оперативной памяти (буфера обмена).	1. Оставление данных в оперативной памяти (буфере обмена).
10. Закрытие утилит.	1 .Закрытие утилит.	1. Завершение работы утилит.	1. Несанкционированная модификация файлов утилит. 2. Оставление работающих в фоновом режиме утилит.

Продолжение таблицы 1

11. Выход из системы.	1. Подготовка к выключению. 2 .Выключение ПК.	1. Выполнение утилит подготовки к выключению.	1. Некорректное завершение работы, которое приводит к автоматическому сохранению данных. 2. Модификация файлов из-за некорректного завершения работы.

IV Выводы

1. Предложена методика систематизации характеристик типовых компьютерных систем, позволяющая учесть их особенности при разработке системы защиты обрабатываемой информации от несанкционированного доступа.
2. Методика заключается в следующем:
   - формализуются этапы подготовки документов в типовой КС;
   - с учетом общих принципов политики безопасности формализуются и детализируются действия пользователей при формировании файлов документов;
   - систематизированным действиям пользователя ставятся в соответствие действия операционной системы и угрозы.
3. Результат применения методики – модель угроз, в основе которой лежат:
   - основные принципы политики безопасности;
   - формализованные действия пользователя при формировании файлов документов;
   - действия операционной системы по обеспечению задач, выполняемых пользователем;
   - угрозы, сопровождающие действия операционной системы.

На основе ранее предложенной политики безопасности [1] и рассмотренной методики систематизации характеристик получена модель угроз для типовой компьютерной системы на основе одномашинного многопользовательского комплекса.

4. Предложенные в статье подходы могут стать основой методики систематизации и для многомашинного многопользовательского комплекса с одновременной обработкой информации с ограниченным доступом.

5. Методику предполагается применить для проведения сравнительного системного анализа операционных систем Windows NT, -2000, Novell Net Ware и Unix с целью оценки соответствия встроенных услуг защиты и аудита предлагаемой политике безопасности.

Литература: 1. Яковив И. Б., Черноног А. А. «Анализ образующих сред типовых компьютерных систем» // Науково-технічний збірник "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні". – Вип. 2. – с. 129–132. – К., 2001. 2. Нормативный документ системы технической защиты «Критерии оценки защищенности информации в компьютерных системах от несанкционированного доступа» от 28. 04. 1999 г. // НД ТЗИ 2.5 – 004 – 99. 3. Нормативный документ системы технической защиты «Классификация автоматизированных систем и стандартные функциональные профили защищенности обрабатываемой информации от несанкционированного доступа» от 28. 04. 1999 г. // НД ТЗИ 2.5 – 004 – 99.

УДК 681.324

КЛАСИФІКАЦІЯ І АНАЛІЗ МОДЕЛЕЙ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ

Ігор Яковів, Олександр Корнейко*, Олександр Черноног*

*Національна академія СБУ, * ВІТІ НТУУ «КПІ»*

Анотація: **Найбільший розвиток теоретичних досліджень в області захисту інформаційних систем отримало формальне моделювання систем і процесів захисту інформації. З метою аналізу забезпечення чіткого розподілу між багаточисельними методами та моделями систем і процесів захисту проведена їх класифікація.**

Summary: **The greatest development of the theoretical researches in the field of a security of information systems has received a formal simulation of systems and processes for the protection of the information. To**